AMENDMENTS TO THE CLAIMS:

1. (Previously Amended) A method to detect unauthorized reconnaissance or scanning of a computer network comprising the acts of:

monitoring communications within the network;

detecting a predefined sequential triplet of TCP/IP protocol set packets flowing within said communications, comprising the steps of:

observing an initial SYN packet originating from a source address;

detecting a next sequential SYN/ACK packet issuing from a target device address in response to the SYN packet; and

detecting a last sequential RST packet originating from the source address in response to the SYN/ACK packet; and

issuing an alert indicating unauthorized scanning if the predefined sequence of packets are each relevant to the source address.

2. (Cancelled)

3. (Currently Amended) The method of claim 1 ~~or claim 2~~ wherein the detecting ~~act~~ further includes~~ the acts of~~:

providing a histogram in which states of the predefined sequence of packets are maintained; and

dynamically updating said histogram as selected ones of the predefined sequence of packets is detected.

4. (Currently Amended) The method of claim 3 wherein the histogram includes a table partitioned into a first field in which source addresses of network devices are kept[~~;~~] and a second field[~~,~~] concatenated to the first field, comprising

initializing or incrementing a state ~~in which a~~ code field ~~representing states in which~~ in response to an order in which packets in the predefined sequence of packets are detected, wherein issuing the alert comprises issuing the alert if the state code field has an alert value.

5-7. (Cancelled) .

8. (Currently Amended) The method of claim ~~1~~ 4 wherein the issuing ~~act~~ further includes ~~the act of~~ sending a message to an administrator.

9. (Currently Amended) The method of claim ~~1~~4 wherein the issuing ~~act~~ further includes ~~the act of~~ blocking future packets ~~from network computers having predefined characteristics~~ comprising the source address, the target device address and a target device port address.

10. (Currently Amended) The method of claim ~~1~~4 wherein ~~the~~ issuing ~~act~~ further includes ~~the act of~~ rate-limiting flows of packets ~~from network devices having predefined characteristics~~ comprising the source address.

11-24. (Cancelled).

25. (Previously Amended) A method to deploy an intrusion detection system on a network device including acts of:

providing an algorithm to detect a predefined sequential triplet of TCP/IP protocol packets; and

generating an alert if the predefined triplet of packets is detected and the triplet packets are each relevant to a source address;

wherein the triplet comprises an initial SYN packet originating from the source address, a next sequential SYN/ACK packet issuing from a target device address in response to the SYN packet, and a last sequential RST packet originating from the source address in response to the SYN/ACK packet.

26. (Previously Amended) The method of claim 25 further including the act of providing a table to record at least one characteristic to identify network devices and state code corresponding to a sequence in which the predefined sequential triplet of packets are received.

27-29. (Cancelled)

30. (Previously Amended) A method to protect devices from malicious attacks launched on a computer network including the acts of:

providing on a device to be protected a software program that monitors packets; and

issuing an alert if a predefined sequential triplet of TCP/IP protocol packets are detected and the triplet packets are each relevant to a source address;

wherein the triplet comprises an initial SYN packet originating from the source address, a next sequential SYN/ACK packet issuing from a target device address in response to the SYN packet, and a last sequential RST packet originating from the source address in response to the SYN/ACK packet.

31-33. (Cancelled).

34. (Currently Amended) The method of claim 30 wherein the software program includes a table containing codes whose values represent detection of one of the predefined set of packets and at least one source address associated with at least one of the codes.

35. (Cancelled)

36. (New) The method of claim 4, wherein each of the predefined sequential triplet packets comprise a source address field, a target device address field, a source port field and a target device port field, and wherein dynamically updating the histogram comprises:

concatenating a source address field, a target device address field, a source port field and a target device port field of a packet of the predefined sequential triplet into the table first and second fields as an ordered four-tuple;

hashing the ordered four-tuple; and

using the hashed ordered four-tuple as a histogram location index.

37. (New) The method of claim 36, wherein detecting the predefined sequential triplet comprises:

concatenating source address, target device address, source port and target device port fields of the SYN packet in a source address-target device address-source port-target device port first order four-tuple and initializing the state code field;

concatenating source address, target device address, source port and target device port fields of the SYN/ACK packet in a reflection of the first order in a target device address-source address-target device port-source port reflected order four-tuple and incrementing the initialized state code field; and

concatenating source address, target device address, source port and target device port fields of the RST packet in a first order four-tuple and incrementing the incremented state code field into the alert value.

38. (New) The method of claim 37, comprising:

starting a purge time period;

purging the state code field upon a lapse of the purge time period.

39. (New) The method of claim 37, wherein detecting the next sequential SYN/ACK packet comprises matching a look-up table key source address to the SYN/ACK source address field.

40. (New) The method of claim 26 further comprising blocking future packets comprising the source address, the target device address and a target device port address.

41 (New) The method of claim 26 further comprising rate-limiting flows of packets comprising the source address.

42. (New) The method of claim 26, wherein each of the predefined sequential triplet packets comprise a source address field, a target device address field, a source port field and a target device port field, comprising dynamically updating a histogram by:

concatenating a source address field, a target device address field, a source port field and a target device port field of a packet of the predefined sequential triplet into a histogram table field as an ordered four-tuple;

hashing the ordered four-tuple; and

using the hashed ordered four-tuple as a histogram location index.

43. (New) The method of claim 42, wherein detecting the predefined sequential triplet comprises:

concatenating source address, target device address, source port and target device port fields of the SYN packet in a source address-target device address-source port-target device port first order four-tuple and initializing the state code;

concatenating source address, target device address, source port and target device port fields of the SYN/ACK packet in a reflection of the first order in a target device address-source address-target device port-source port reflected order four-tuple and incrementing the initialized state code; and concatenating source address, target device address, source port and target device port fields of the RST packet in a first order four-tuple and incrementing the incremented state code into an alert value.

44. (New) The method of claim 43, comprising:
starting a purge time period;
purging the state code upon a lapse of the purge time period.

45. (New) The method of claim 43, wherein detecting the next sequential SYN/ACK packet comprises matching a look-up table key source address to the SYN/ACK source address field.

46. (New) The method of claim 35 further comprising blocking future packets comprising the source address, the target device address and a target device port address.

47 (New) The method of claim 35 further comprising rate-limiting flows of packets comprising the source address.

48. (New) The method of claim 35, wherein each of the predefined sequential triplet packets comprise a source address field, a target device address field, a source port field and a target device port field, comprising dynamically updating a histogram by:

concatenating a source address field, a target device address field, a source port field and a target device port field of a packet of the predefined sequential triplet into a histogram table field as an ordered four-tuple;

hashing the ordered four-tuple; and

using the hashed ordered four-tuple as a histogram location index.

49. (New) The method of claim 48, wherein detecting the predefined sequential triplet comprises:

concatenating source address, target device address, source port and target device port fields of the SYN packet in a source address-target device address-source port-target device port first order four-tuple and initializing a state code;

concatenating source address, target device address, source port and target device port fields of the SYN/ACK packet in a reflection of the first order in a target device address-source address-target device port-source port reflected order four-tuple and incrementing the initialized state code; and

concatenating source address, target device address, source port and target device port fields of the RST packet in a first order four-tuple and incrementing the incremented state code into an alert value.

50. (New) The method of claim 49, comprising:
starting a purge time period;
purging the state code upon a lapse of the purge time period.

51. (New) The method of claim 49, wherein detecting the next sequential SYN/ACK packet comprises matching a look-up table key source address to the SYN/ACK source address field.